Maryland Asset Management Policy

Last Updated: 01/31/2017

Contents

1.0 Purpose

Compiling and maintaining inventory and accountability of assets is an important aspect of risk management. According to the *Security Assessment Policy*, each asset must be assigned a security category based on its perceived level of confidentiality, integrity, and availability, and it is the role of **asset management** to inventory, account for, and track these assets. The Maryland Department of Information Technology (DoIT) will utilize baseline controls and standards established by NIST SP 800-53R4 and guidance provided by SP 800-53AR4 and SP 800-60R1.

2.0 Document and Review History

This policy supersedes the Maryland Information Security Policy v3.1 (2013) Section 3.0: Asset Management and any related policy regarding asset management declared prior to the 2017 Cybersecurity Program Policy. This document will be reviewed annually and is subject to revision.

Date	Version	Policy Updates	Approved By:
01/31/2017	v1.0	Initial Publication	Maryland CISO

3.0 Applicability and Audience

This policy is applicable to all **Information Technology (IT) assets** utilized by any agency supported by, or under the policy authority of, the Maryland Department of Information Technology, i.e., any agency of the Maryland Executive Branch of government.

4.0 Policy

This policy describes an overall strategy to implement asset management processes within the Maryland Department of Information Technology infrastructure as well as State agencies managing their own assets outside of the DoIT Enterprise. Agency IT assets within the DoIT Enterprise will be managed by the Enterprise policy, associated processes, and personnel. Non-Enterprise agencies (those yet to navigate the onboarding process; those exempted from certain functions of the Enterprise; and those agencies not under the authority of the State Executive Branch) will manage their own IT assets through an Assigned Asset Manager rather than the Enterprise Asset Manager.

Supporting and related policies are shown in section 6.0 below.

4.1 General Requirements

Maryland DoIT shall assign an Enterprise Asset Manager to maintain an accurate and timely inventory of all trackable information technology assets within the DoIT Enterprise. The Enterprise Asset Manager, or agency Assigned Asset Managers, will observe the requirements shown in section 4.1.1 below.

4.1.1 Minimum Requirements for Asset Management

#	Name	Requirement
A	Asset Inventory and Tracking	Track and account for IT assets, including: physical devices, software, and data IT assets (as defined in section 7.0).
B	Annual Audit	Conduct an annual physical audit of IT assets and reconcile the audit with the IT asset inventory. Investigate and resolve discrepancies between the physical audit of IT assets and the IT asset inventory, including software licenses.
C	Periodic Updates	Update and maintain the asset inventory as assets are acquired, configured, deployed, or disposed of throughout the asset lifecycle. Non-Enterprise agencies under policy authority of DoIT will report on their assets to the Enterprise Asset Manager for auditing purposes.
D	Automated Asset Inventory	Implement an automated mechanism to support tracking of information system assets, where possible.

4.2 Types of Assets

4.2.2 Physical IT Assets

Physical IT assets will be actively tracked and accounted for by the Enterprise Asset Manager or agency Assigned Asset Manager, who will maintain at least the following information shown in the table below regarding physical IT assets.

#	Name	Requirement
A	Physical Assets	Maintain an inventory of physical IT assets.
B	Contacts	Identify and maintain contact information for both the primary user of the device, and the responsible system administrator or IT group.
C	Type	Identify the device type: ▪ Desktop ▪ Laptop ▪ Tablet ▪ Mobile Phone ▪ IP Phone ▪ Server (including virtual machines) ▪ Security Appliance ▪ Storage Appliance ▪ Network Device ▪ Supercomputer ▪ Printer/Scanner/Fax ▪ Media (i.e. USB or external hard drives) ▪ SCADA Systems ▪ Other: <specify>
D	Hardware Identification	Identify and record the device manufacturer, make, model and serial number.
E	Physical Location	▪ Identify the physical location of the device. ▪ If the device is primarily stationary, include building address and room number ▪ If the device is rack mounted, include rack # ▪ Identify if the device is mobile
F	Logical Identification	▪ Record logical identifiers for the device.

#	Name	Requirement
		▪ IP address(es) (if static) ▪ Host name ▪ Domain membership ▪ MAC address(es)
G	Operating System	Record the type and version of the operating system installed on the device.
H	Security Categorization	Record the security categorization of the device. Include notes as to the basic reason behind the categorization (see *Security Assessment Policy* for categorization assignments).
I	Purpose	Record the general purpose of the device.
J	Asset Tag	Each physical asset will be affixed with an asset tag, which will include a unique asset identifier. Media assets like CD/DVDs will be tracked as software media under Section 4.2.3.
K	Date	Record the date on which the item was entered into and/or removed from inventory.

4.2.3 Software Assets

The Enterprise Asset Manager or agency Assigned Asset Manager shall maintain a **Software Media Library** to control access to State purchased software and licenses as well as track when software or licenses are being utilized within the Enterprise or Agency. The library will store and track software and licenses, burnable CD/DVDs or other disposable media (see *Media Protection Policy*), and non-disposable media such as USB memory sticks and external hard drives following the requirements shown in the table below.

#	Name	Requirement
A	Software Assets	Maintain an inventory of all software used within the Enterprise/Agency including any associated licenses.
B	Issue Control Number	Identify and maintain a unique asset identifier that will allow tracking physical copies of software or disposable media. See *Media Protection Policy* regarding tracking and accounting for media such as burnable CD/DVDs and vendor software disks.
C	Approved Software	Agencies shall maintain a list of approved applications and services for all managed computer systems. This list shall include: ▪ Vendor ▪ Make ▪ Model ▪ Version Exception: Specialized appliances for which the agency has no control at the operating system level.
D	Installed Software by Device	Use an automated tool to identify the software installed on any given computer system.

#	Name	Requirement
E	Licensing	Maintain a list of all software licenses, and track the differential between the number of owned licenses and the number of deployed instances of the software.

4.2.4 Data Assets

The Enterprise Asset Manager or agency Assigned Asset Manager shall identify, track, and account for ownership of assets containing or transmitting confidential data; such assets will be identified in the organization's Organizational Risk Management Report (see *Security Assessment Policy*).

Any data categorized as Confidential will be managed and protected with controls at the NIST 800-53R4 Moderate or High baseline. The Enterprise or agency Assigned Asset Manager shall manage the confidential-data-related assets as shown in the table below.

#	Name	Requirement
A	Data Assets	Identify and maintain an accurate list of confidential data.
B	Confidential Data Types	Maintain a list of confidential data that is processed, stored, or transmitted by the agency. This will include data that is specific to an agency's business/mission areas (such as law enforcement), as well as regulated data types, including but not limited to: ▪ Heath Information (HIPAA) ▪ Payment Card Data (PCI DSS) ▪ Personally Identifiable Information (PII) ▪ Federal Tax Information (IRS 1075)
C	Confidential Data: Major Repositories	Identify all major repositories of confidential data. Repositories will be identified by: ▪ Host name ▪ Asset Tag ▪ Stored, confidential data type(s) (See 4.1.4 (B)) ▪ Volume of records (Estimate) per data type ▪ Encryption status of data at rest
D	Confidential Data: Major Transit Routes	Identify all major network transit routes, to and from major confidential data repositories, documented in the form of a topology diagram.
E	Confidential Data Detection	Implement an automated mechanism for scanning and detecting confidential data across computer systems in the agency.

Further information on confidential data can be found in the *Public and Confidential Information Policy*.

4.3 Asset Security Categorization

The asset security categorization is outlined within the *Security Assessment Policy*.

5.0 Exemptions

This policy is established for use within the DoIT Enterprise. If an agency under the policy authority of DoIT requires an exemption from this policy, then that agency must submit a DoIT Policy Exemption Request Form and clearly articulate the reason for the exemption. An operational risk assessment will be conducted to identify the risks and the agency's mitigation strategy associated with this exemption. If the agency can accept the risk, an exemption to this policy may be granted.

6.0 Policy Mandate and References

The Cybersecurity Program Policy mandates this policy. Other related policies include:

- Configuration Management Policy
- HIPAA Security Rule Policy
- Media Protection Policy
- Network Architecture and Documentation Policy
- PCI DSS Compliance Policy
- Public and Confidential Information Policy
- Security Assessment Policy

7.0 Definitions

Term	Definition
Asset Management	The method for identifying, procuring, maintaining, tracking, and disposing of all information technology assets.
Information Technology (IT) Assets	Assets typically include: ▪ Physical devices such as servers, virtual servers, workstations (desktops, laptops, and thin clients), printers/scanners, VoIP systems, telecomm assets, security (e.g., CCTV or entry control systems), SCADA-type systems, and standalone/offline systems; ▪ Software such as purchased applications and programs, associated licenses; and ▪ Data, such as information or aggregate digital content processed, stored, or transmitted by IT systems, which includes confidential information (Personally Identifiable Information (PII), Privileged Information, and Sensitive Information).
Software Media Library	A central repository for managing and inventorying physical copies of organizationally approved software, software licenses, and disposable media such as CD/DVDs and approved memory devices such as USB Flash Drives.

8.0 Enforcement

The Maryland Department of Information Technology is responsible for information technology asset management of Enterprise onboarded agencies. DoIT will manage assets according to established requirements as outlined in section 4.0 unless an agency has completed a Policy Exemption Request Form and received approval from DoIT. Agencies under the policy authority

of DoIT, but not under direct management, must manage assets so as to meet the requirements established in section 4.0 and provide an inventory report (annually) to the DoIT Enterprise Asset Manager for auditing purposes, unless a Policy Exemption Request has been approved by DoIT. This report must include the physical audit of IT assets reconciled against the IT asset inventory. Discrepancies between the physical audit of IT assets and the IT asset inventory may be considered a security violation.

If DoIT determines that an agency is not compliant with the *Asset Management Policy*, the agency will be given sixty (60) days to become compliant according to the requirements in this policy. After such time, if the agency remains out of compliance the Secretary of Information Technology will be notified and remediation will be mandated.

Any personnel attempting to circumvent asset inventory, such as stealing property — including assets assigned for disposal — or intentionally omitting, failing to record, or excluding assets from inventory will be investigated and subject to disciplinary action, which may include written notice, suspension, termination, and possible criminal and/or civil penalties.